

# Herausforderungen an den Datenschutz und die Sicherheit nutzerbezogener Verbrauchsdaten

## -Datenschutzfragen zum Messsystem-



# Datenschutz und -Sicherheit



## Ziel

Die schutzwürdigen Interessen der Betroffenen in Bezug auf ihr Recht auf informationelle Selbstbestimmung müssen gewahrt und sichergestellt werden

**Niemand kann unberechtigterweise Informationen über (das Nutzungsverhalten der) Letztverbraucher erlangen.**

Vertraulichkeit, Integrität, Intervenierbarkeit, Transparenz, Nichtverkettbarkeit sowie Verfügbarkeit der Daten müssen gewahrt und sichergestellt werden.

## Umsetzung

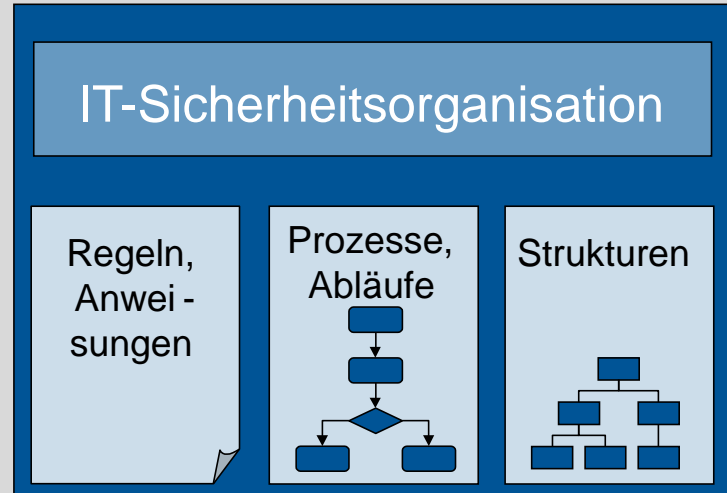
### **Privacy & Security by Design**

Die Gewährleistung von Datenschutz und Datensicherheit muss bereits bei der Konzeption und Gestaltung der Systeme erfolgen.

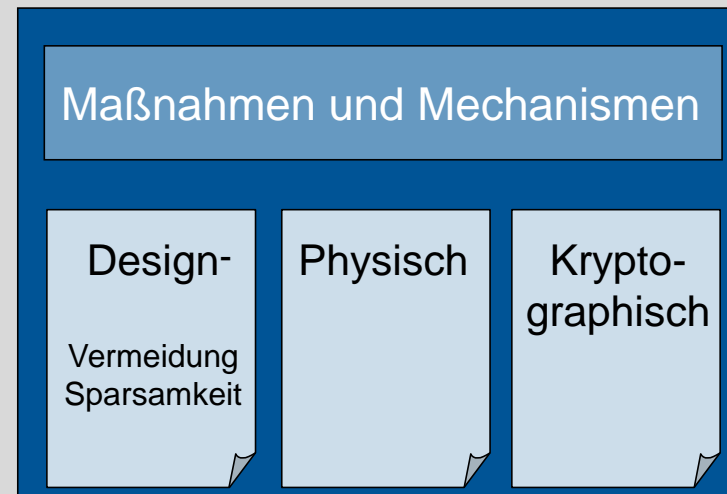
Von Anfang an müssen die Datenverarbeitungssysteme ein integriertes Datenschutzmanagementsystem enthalten und technische Maßnahmen der Datensicherheit vorsehen.

# Hilfsmittel zur Umsetzung

Organisatorisch

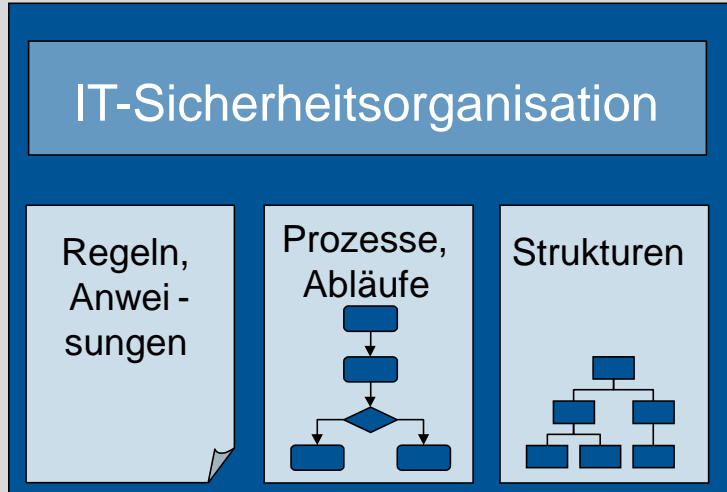


Technisch



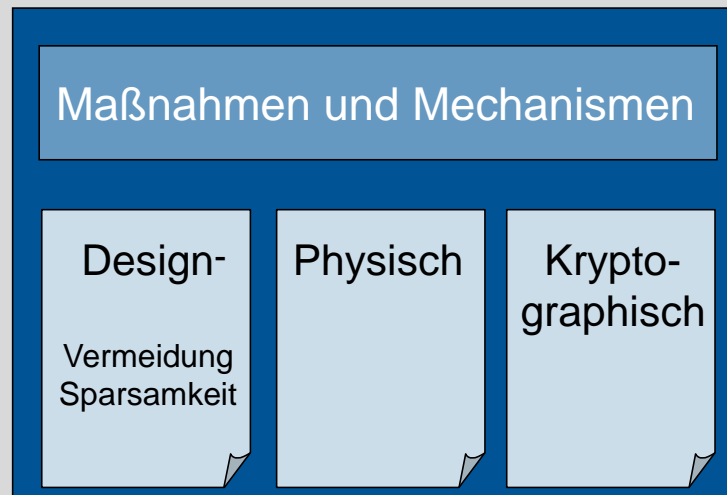
# Herausforderungen

## Organisatorisch



- Verständnis
- Vertrauen
- Komplexität

## Technisch



- Komplexität
- Umgebung
- Rechenleistung
- Beweisbarkeit

# Herausforderungen an die Kryptographie



- Initialisierung des Kryptosystems
  - **Geschwindigkeit**
  - **Datengröße** (Schlüssellänge)
- Ausführung eines Kryptosystems
  - **Geschwindigkeit**
  - **Datengröße**
  - Integration in Protokolle (Latenz)

## Herausforderungen an die Sicherheit des Kryptosystems!

- Komplexität/Sicherheit des Verfahrens
- Auswahl der Parameter des Verfahrens
- Protokoll-/Anwendungsfehler
- Implementierungsfehler

# Herausforderungen an die Kryptographie

## Komplexität/Sicherheit

- abhängig von **Schlüssellänge**
- **Sicherheitsvermutungen**
  - auf Basis von Erfahrungen oder
  - „schwierigen“ Problemen
- nicht beweisbar

## Beispiele für Sicherheitsvermutungen:

- RSA: Schwieriges Problem: **Faktorisierung**
  - Gegeben  $n = pq$ , wobei  $p, q$  Primzahl. Man finde Primfaktorzerlegung  $p, q$ .
- ElGamal: Schwieriges Problem: **Diskrete Logarithmen**
  - Gegeben endliche Gruppe  $G$ , gegeben  $x, y \in G$  mit  $y = x^n$ . Man finde  $n$ .
    - Verwendete Gruppen: Ganze Zahlen modulo  $p$ , Elliptische Kurven

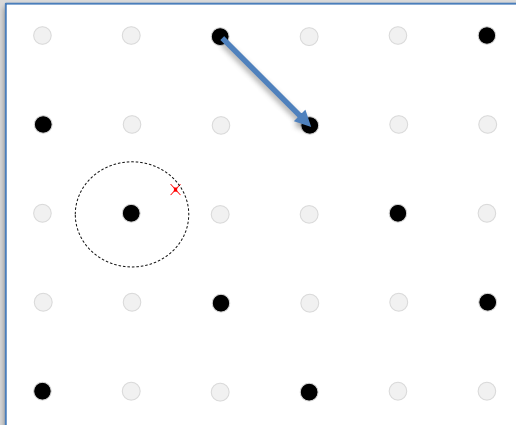
# Eine neue Herausforderung: Quantencomputer

- Grovers Algorithmus
  - Suche in einer unsortierten Liste mit N Einträgen
  - Klassisch:  $O(n)$
  - Quantenalgorithmus:  $O(\sqrt{n})$
  - **Grovers Algorithmus verdoppelt die Länge aller Passwörter/Schlüssel, die man brechen kann**
- Shors Algorithmus
  - Quanten-Fouriertransformation in endlichen Gruppen
  - **Shors Algorithmus liefert ausgerechnet eine effiziente Lösung (in Polynomialzeit) für Faktorisierung von ganzen Zahlen und Diskrete Logarithmen**

**Quantencomputer brechen viele zur Zeit populären  
Kryptoverfahren**

# Alternative: Kryptographie mit Gittern

- Kryptoverfahren basierend auf „neuen“ schwierigen Problemen, die bisher nicht von Quantencomputern effizient gelöst werden können:



- SVP: Shortest Vector Problem
- CVP: Closest Vector Problem
  - Verschlüsselung: Addition speziell präparierter Vektoren
  - Entschlüsselung: Invertierung der Addition durch Kenntnisse über die speziell präparierten Vektoren

- $\pm$  Starke Sicherheitsvermutung (dann allerdings nicht effizient)
- $\pm$  Sehr effiziente Ver- und Entschlüsselung (dann allerdings keine starken Sicherheitsvermutungen)





**FH Bielefeld**  
University of  
Applied Sciences

- Zusammenhang zwischen Gittern und Polynomen, z.B.

$$\mathbb{Z}_n \cong \mathbb{Z}[X] / \langle f \rangle$$

- Schlüssel sind Polynome, verwandt mit Gitterreduktion
- Parameter:
  - $N, p, q, d_f, d_g, d_m$
  - Parametrisierung für die optimale Konfiguration schwierig
  - $d_f, d_g, N$  bestimmt den Schlüsselraum
  - $d_m$  bestimmt den Zufallsanteil jeder Nachricht
  - $N$  bestimmt ebenfalls die mögliche Nachrichtenlänge
  - $p$  legt die Kodierung der zu verschlüsselnden Nachrichten fest
  - Mit  $q$  wächst die Größe des Verschlüsselungsraums proportional

**Aufgabe:**

**Optimale Parameter: Sicherheit / Geschwindigkeit**

# Optimierte Parameter für unser Messsystem

- $$\binom{N}{d_f} \cdot \binom{N - d_f}{d_f} \cdot \binom{N}{d_g} \cdot \binom{N - d_g}{d_g} = 4.9 \cdot 10^{136}$$

- $N = 223$
- $p = 3$
- $q = 256$
- $d_f = 30$
- $d_g = 25$
- $d_m = 15$
- Sehr großer Schlüsselraum
- Ver- und Entschlüsselung in unter 300 ms möglich
- Effizient implementierbar in leistungsschwacher HW (16 Bit)

# Zusammenfassung

- Anforderungen an Organisation und Technik
- Konkreteres Beispiel: Technik → Kryptographie → NTRU
- Ausblick:
  - Sicherheitsanalyse verfeinern
  - Weitere Optimierung der Implementierung
    - Spezialfälle der Gitter